9/11/2565

1. **ux/ui cx**

ui is subset of ux, ux is subset of cx. => ui เป็นส่วนหนึ่งของ ux และ ux เป็นส่วนหนึ่งของ cx

**CX -> customer experience** => มี CRM, CEM

**CX(การทำให้ลูกค้ามีความรู้สึกที่ดีต่อองค์กรและมีความไว้วางใจแก่องค์กร)**

->การนำข้อมูลลูกค้าที่เป็นพฤติกรรมการซื้อ ไลฟ์สไตล์ ความชอบ ช่อวทางในโซเชียลมิเดีย และ feedbackของลูกค้ามาวิเคราะห์

เพื่อนำเสนอสินค้าหรือผลิตภัณฑ์ที่ตอบสนองความต้องการของลูกค้าได้ และสามารถหาลูกค้าใหม่ๆได้มากยิ่งขึ้น ทำให้ลูกค้ารู้สึกดีกลับไปไปและมีประสบการณเชิงบวกต่อแบรนด์

**CX ที่ดี->** 1.เข้าใจลูกค้า

2.ทำให้ลูกค้ารู้สึกดีกับสินค้าบริการ

3.บริการหลังการขาย

4.รับฟังความเห็นจากลูกค้า

5.สร้างระบบบริหารงานที่ดี

**ความเหมือน และ ความแตกต่างระหว่าง CRM และ CEM**

**ความเหมือน:** ทั้ง CEM และ CRM ใช้วิธีการนำ Data มาต่อยอดเพื่อให้ลูกค้าได้รับสินค้า และ บริการที่ดีที่สุด ตอบโจทย์ที่สุดแบบเฉพาะบุคคล เพื่อรักษาความสัมพันธ์ที่ดีระหว่างแบรนด์ และ ลูกค้าให้เติบโต

**ความแตกต่าง:** CEM โฟกัสที่การสร้างประสบการณ์ในเชิงบวกในทุกครั้งที่มีการติดต่อกับลูกค้า โดยใช้ข้อมูลเชิงคุณภาพในรูปแบบ Customer Touch Point (การที่ลูกค้ามีปฏิสัมพันธ์ต่อแบรนด์ในทุกรูปแบบ) ทั้งในรูปแบบหน้าร้าน และ แบบดิจิทัล แต่ CRM จะเป็นการบริหารความสัมพันธ์ของลูกค้า ที่ใช้ Data เชิงปริมาณมาทำแคมเปญ โดยเน้นสร้างผลลัพธ์

**ux->user experience** => ออกแบบที่เน้นความรู้สึกของผู้ใช้ ให้รู้สึกชอบหรือให้รู้สึกแบบที่ผลิตภัณฑ์อยากให้เกิด เช่นออกแบบคอนเทนต์ เนื้อหาของผลิตภัณฑ์

tool ->design thinking=> 1.empathize

2.define

3.ideate

4.prototype

5.test

->lean

->lean startup

->lean ux

->service design

->sprint design

**###การทำ usability ทำให้ลูกค้าใช้งานง่ายไม่จำเป็นต้องใช้คู่มือ###**

**ui-> user interface** => ส่วนที่ติดต่อกับ user หรือหน้าตาของผลิตภัณฑ์

**tool -> UI/UX => figma**

**2. owasp->Open Web Application Security Project => (มาตรฐานความปลอดภัยของ web application)**

ไว้ตรวจสอบว่า web application ว่ามีความปลอดภัยมากน้อยแค่ไหน หรือเครื่องมือตรวจสอบช่องโหว่ของ web application OWASP จะมีโครงการหนึ่งที่จัดอันดับ 10 ความเสี่ยงด้านความปลอดภัย ทั้งทางด้าน การโจมตีทั้งแอปพลิเคชั่น IOT , Cloud ต่างๆ เป็นต้น

ที่ถูกเรียกว่า **OWASP TOP 10(2021)** ประกอบด้วย

**1. Broken Object Level Authorization (สิทธิ์การเข้าถึงจาก login)** =>

คือ เวลาที่ API มีการอ้างอิงไปที่ Object อะไรบางอย่าง ด้วยค่า ID หรือ token ก็ได้

จะต้องมีการตรวจสอบสิทธิ์ ว่าผู้ใช้งานที่เรียก Object นั้น ๆ มีสิทธิ์ ในการอ่านหรือแก้ไขข้อมูลปลายทางที่ขอหรือเปล่า ถ้าการตรวจสอบนี้ไม่มี หรือไม่ถูกต้อง แฮกเกอร์ก็อาจสามารถอ่านหรือ แก้ไขข้อมูลที่ตนเองไม่ควรจะมีสิทธิ์ได้(สิทธิ์ที่เท่ากัน)

**2. Broken User Authentication(ยืนยันตัวตนว่าเป็นใคร)** =>

คือการโจมตีที่เกี่ยวกับการ login โดยใช้ Username และ Password หรือ การใช้ Login Key หรือ การใช้ session token

**3. Excessive Data Exposure** => การที่ API ตอบข้อมูลมามาก เกินกว่าที่จะต้องนำไปใช้งานจริง

**4. Lack of Resources & Rate Limiting** =>

ไม่มีการลิมิตจำนวนการ call เช่นไม่มีการตั้ง time out หรือตั้ง time out ไว้นานจะทำให้ค้าง หรือ time out อาจจะทำให้ทำงานไม่เสร็จ ดังนั้นจึงจำเป็นต้องตั้งลิมิตของขนาดและความถี่

**5. Broken Function Level Authorization [คล้าย 1 แต่จะเป็นการทำงานในสิทธิ์ที่สูงกว่า]** => เช่นการทำงานที่ user login เข้ามาแล้วสามารถเปลี่ยน path ให้เป็น admin หรือการเปลี่ยนแปลงเพื่อให้ทำงานที่มีสิทธิ์การทำงานที่ต่างจากตนมีสิทธิ์ได้

**6. Mass Assignment** => ช่องโหว่ที่ API ยอมรับค่าเกินกว่าที่ควรจะเป็นจริง ๆ ถ้าหากถูกใส่เข้าไป เช่น การใส่ properties ที่เกินกว่าที่ควรจะเป็น ตัวอย่างเช่น การโอนเงินโดยส่งค่าที่แก้ไขหรือเพิ่ม properties status เป็น approve แล้วก้มีการยอมรับจากระบบหลังบ้าน

**7. Security Misconfiguration** => คือมีการ Config ทุกตำแหน่งการใช้งาน/การทำงานที่ไม่ Security พอ หรือการ patches ที่ช้าเกินไปและไม่ Up-to-date

**8. Injection** => เกิดขึ้นได้ในกรณีที่ API รับค่าจากผู้ใช้งานมาประมวลผลอย่างงไม่ปลอดภัย โดยเฉพาะอย่างยิ่ง ไม่ได้ตรวจสอบค่าที่รับเข้ามาก่อน มีหลายประเภทเช่น SQL, NoSQL, Command etc. หรือไม่มีการกำหนดรูปแบบการรับค่า request จากผู้ใช้

**9. Improper Assets Management** => เป็นความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการดูแล API ไม่ดีอย่างเพียงพอ (การป้องกันคือทำ Doc / inventory ว่ามีทรัพสินอะไรบ้าง และมีอยู่ที่ได้)

**10. Insufficient Logging & Monitoring** => คือการมี log ไม่เพียงพอ / ไม่มีการ Monitoring สม่ำเสมอ